PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L 9/30 — A1

(11) Numéro de publication internationale: **WO 00/59157**

(43) Date de publication internationale: 5 octobre 2000 (05.10.00)

(21) Numéro de la demande internationale: PCT/FR00/00723

(22) Date de dépôt international: 22 mars 2000 (22.03.00)

(30) Données relatives à la priorité:
99/03920 26 mars 1999 (26.03.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS [FR/FR]; Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F–13881 Gémenos (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(US seulement)*: CORON, Jean–Sébastien [FR/FR]; 4, rue Léon de Lagrange, F–75015 Paris (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus, Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F–13881 Gémenos (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.

(54) Title: COUNTERMEASURE METHOD IN AN ELECTRIC COMPONENT IMPLEMENTING AN ELLIPTICAL CURVE TYPE PUBLIC KEY CRYPTOGRAPHY ALGORITHM

(54) Titre: PROCEDE DE CONTRE–MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE DE TYPE COURBE ELLIPTIQUE

(57) Abstract

The invention relates to a countermeasure method in an electronic component implementing an elliptical curve based public key cryptography algorithm, comprising the calculation of a new decryption integer d' such as the decryption of an encrypted message with the aid of a decryption algorithm on the basis of a private key d and the number of points n of said elliptical curve whereby the same result is achieved with d' as with d, by performing the operation Q=d*P, whereby P is a point of the curve. The inventive measure is characterized in that it comprises four steps: 1) a security parameter s is determined, whereby in practice it is impossible to take s as a neighbour of 30, 2) a random number k ranging from 0–21s is drawn, 3) the integer d'=d+k*n is calculated, 4) Q=d'.P is calculated.

(57) Abrégé

La présente invention concerne un procédé de contre–mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé publique basé sur l'utilisation des courbes elliptiques consistant à calculer à partir de la clé privée d et du nombre de points n de ladite courbe elliptique un nouvel entier de déchiffrement d' tel que le déchiffrement d'un message chiffré quelconque, au moyen d'un algorithme de déchiffrement, avec d' donne le même résultat qu'avec d, en réalisant l'opération Q=d*P, P étant un point de la courbe, procédé caractérisé en ce qu'il comprend quatre étapes: 1) détermination d'un paramètre de sécurité s, dans la pratique on peut prendre s voisin de 30; 2) tirage d'un nombre aléatoire k compris entre 0 et 21s; 3) calcul de l'entier d'=d+k*n; 4) calcul de Q=d'.P.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie
AM	Arménie
AT	Autriche
AU	Australie
AZ	Azerbaïdjan
BA	Bosnie-Herzégovine
BB	Barbade
BE	Belgique
BF	Burkina Faso
BG	Bulgarie
BJ	Bénin
BR	Brésil
BY	Bélarus
CA	Canada
CF	République centrafricaine
CG	Congo
CH	Suisse
CI	Côte d'Ivoire
CM	Cameroun
CN	Chine
CU	Cuba
CZ	République tchèque
DE	Allemagne
DK	Danemark
EE	Estonie
ES	Espagne
FI	Finlande
FR	France
GA	Gabon
GB	Royaume-Uni
GE	Géorgie
GH	Ghana
GN	Guinée
GR	Grèce
HU	Hongrie
IE	Irlande
IL	Israël
IS	Islande
IT	Italie
JP	Japon
KE	Kenya
KG	Kirghizistan
KP	République populaire démocratique de Corée
KR	République de Corée
KZ	Kazakstan
LC	Sainte-Lucie
LI	Liechtenstein
LK	Sri Lanka
LR	Libéria
LS	Lesotho
LT	Lituanie
LU	Luxembourg
LV	Lettonie
MC	Monaco
MD	République de Moldova
MG	Madagascar
MK	Ex-République yougoslave de Macédoine
ML	Mali
MN	Mongolie
MR	Mauritanie
MW	Malawi
MX	Mexique
NE	Niger
NL	Pays-Bas
NO	Norvège
NZ	Nouvelle-Zélande
PL	Pologne
PT	Portugal
RO	Roumanie
RU	Fédération de Russie
SD	Soudan
SE	Suède
SG	Singapour
SI	Slovénie
SK	Slovaquie
SN	Sénégal
SZ	Swaziland
TD	Tchad
TG	Togo
TJ	Tadjikistan
TM	Turkménistan
TR	Turquie
TT	Trinité-et-Tobago
UA	Ukraine
UG	Ouganda
US	Etats-Unis d'Amérique
UZ	Ouzbékistan
VN	Viet Nam
YU	Yougoslavie
ZW	Zimbabwe

PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN ŒUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE DE TYPE COURBE ELLIPTIQUE

La présente invention concerne un procédé de contre-mesure dans un composant électronique mettant en œuvre un algorithme de chiffrement à clé publique de type courbe elliptique

Dans le modèle classique de la cryptographie à clef secrète, deux personnes désirant communiquer par l'intermédiaire d'un canal non sécurisé doivent au préalable se mettre d'accord sur une clé secrète de chiffrement K. La fonction de chiffrement et la fonction de déchiffrement utilisent la même clef K. L'inconvénient du système de chiffrement à clé secrète est que ledit système requiert la communication préalable de la clé K entre les deux personnes par l'intermédiaire d'un canal sécurisé, avant qu'un quelconque message chiffré ne soit envoyé à travers le canal non sécurisé. Dans la pratique, il est généralement difficile de trouver un canal de communication parfaitement sécurisé, surtout si la distance séparant les deux personnes est importante. On entend par canal sécurisé un canal pour lequel il est impossible de connaître ou de modifier les informations qui transitent par ledit canal. Un tel canal sécurisé peut être réalisé par un câble reliant deux terminaux, possédés par les deux dites personnes.

Le concept de cryptographie à clef publique fut inventé par Whitfield DIFFIE et Martin HELLMAN en 1976. La cryptographie à clef publique permet de résoudre le problème de la distribution des clefs à travers un canal non sécurisé. Le principe de la cryptographie à clef publique consiste à utiliser une paire de clefs, une clef publique de chiffrement et une clef privée de déchiffrement. Il doit être calculatoirement infaisable de trouver la clef privée de déchiffrement à partir de la clef publique de chiffrement. Une personne A désirant communiquer une information à une personne B utilise la clef publique de chiffrement de la personne B. Seule la personne B possède la clef privée associée à sa clef publique. Seule la personne B est donc capable de déchiffrer le message qui lui est adressé.

Un autre avantage de la cryptographie à clé publique sur la cryptographie à clé secrète est que la cryptographie à clef publique permet l'authentification par l'utilisation de signature électronique.

La première réalisation de schéma de chiffrement à clef publique fut mis au point en 1977 par Rivest, Shamir et Adleman, qui ont inventé le système de chiffrement RSA. La sécurité de RSA repose sur la difficulté de factoriser un grand nombre qui est le produit de deux nombres premiers.

Depuis, de nombreux systèmes de chiffrement à clef publique ont été proposés, dont la sécurité repose sur différents problèmes calculatoires : (cette liste n'est pas exhaustive).

- Sac à dos de Merckle-Hellman :

  Ce système de chiffrement est basé sur la difficulté du problème de la somme de sous-ensembles.

- McEliece :

  Ce système de chiffrement est basé sur la théorie des codes algébriques. Il est basé sur le problème du décodage de codes linéaires.

- ElGamal :

  Ce système de chiffrement est basé sur la difficulté du logarithme discret dans un corps fini.

- Courbes elliptiques :

  Le système de chiffrement à courbe elliptique constitue une modification de systèmes cryptographiques existant pour les appliquer au domaine des courbes elliptiques.

L'utilisation de courbes elliptiques dans des systèmes cryptographiques fut proposé indépendamment par Victor Miller et Neal Koblitz en 1985. Les applications réelles des courbes elliptiques ont été envisagées au début des années 1990.

L'avantage de cryptosystèmes à base de courbe elliptique est qu'ils fournissent une sécurité équivalente aux autres cryptosystèmes mais avec des tailles de clef moindres. Ce gain en taille de clé implique une diminution des besoins en mémoire et une réduction des temps de calcul, ce qui rend l'utilisation des courbes elliptiques particulièrement adaptées pour des applications de type carte à puce.

Une courbe elliptique sur un corps fini GF(q^n) (q étant un nombre premier et n un entier) est l'ensemble des points (x,y) avec x l'abscisse et y l'ordonnée appartenant à GF(q^n) solution de l'équation :

$$y^2=x^3+ax+b$$

si q est supérieur ou égal à 3 et

$$y^2+x*y=x^3+a*x^2+b$$

si q=2.

Les deux classes de courbes élliptiques les plus utilisées en cryptographie sont les classes suivantes :

1) Courbes définies sur le corps fini GF(p) (ensemble des entiers modulo p, p étant un nombre premier) ayant pour équation:

$$y^2=x^3+ax=b$$

2) Courbes elliptiques sur le corps fini GF(2^n) ayant pour équation y^2+xy=x^3+ax^2+b

Pour chacune de ces deux classes de courbes, on définit une opération d'addition de points: étant donné deux points P et Q, la somme R=P+Q est un point de la courbe, dont les coordonnées s'expriment à l'aide des coordonnées des points P et Q suivant des formules dont l'expression est donnée dans l'ouvrage « Elliptic Curve public key cryptosystem » par Alfred J. Menezes.

Cette opération d'addition permet de définir une opération de multiplication scalaire: étant donné un point P appartenant à une courbe elliptique et un entier d, le résultat de la multiplication scalaire de P par un point d tel que Q=d.P=P+PP....+P d fois.

La sécurité des algorithmes de cryptographie sur courbes elliptiques est basée sur la difficulté du logarithme discret sur courbes elliptiques, ledit problème consistant à partir de deux points Q et P appartenant à une courbe elliptique E, de trouver, s'il existe, un entier x tel que Q=x.P

Il existe de nombreux algorithmes cryptographiques basés sur le problème du logarithme discret.

Ces algorithmes sont facilement transposables aux courbes elliptiques. Ainsi, il est possible de mettre en œuvre des algorithmes assurant l'authentification, la confidentialité, le contrôle d'intégrité et l'échange de clé.

Un point commun à la plupart des algorithmes cryptographiques basés sur les courbes elliptiques est qu'ils comprennent comme paramètre une courbe elliptique définie sur un corps fini et un point P appartenant à cette courbe elliptique. La clé privée est un entier d choisi aléatoirement. La clef publique est un point de la courbe Q tel que Q=d.P. Ces algorithmes cryptographiques font généralement intervenir une multiplication scalaire dans le calcul d'un point R=d.T où d est la clef secrète.

Dans ce paragraphe, on décrit un algorithme de chiffrement à base de courbe elliptique. Ce schéma est analogue au schéma de chiffrement d'El Gamal. Un message m est chiffré de la manière suivante :

Le chiffreur choisit un entier k aléatoirement et calcule les points k.P=(x1,y1) et k.Q=(x2,y2) de la courbe, et l'entier c= x2 + m. Le chiffré de m est le triplet (x1,y1,c).
Le déchiffreur qui possède d déchiffre m en calculant :
(x'2,y'2)=d(x1,y1) et m=c-x'2

Pour réaliser les multiplications scalaires nécessaires dans les procédé de calcul décrits précédemment, plusieurs algorithmes existent :

Algorithme " double and add " ;
Algorithme " addition-soustraction "
Algorithme avec chaînes d'addition ;
Algorithme avec fenêtre ;
Algorithme avec représentation signée ;

Cette liste n'est pas exhaustive. L'algorithme le plus simple et le plus utilisé est l'algorithme " double and add ". L'algorithme " double and add " prend en entrée un point P appartenant à une courbe elliptique donnée et un entier d. L'entier d est noté d=(d(t),d(t-1),…, d(0)), où (d(t),d(t-1),…,d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. L'algorithme retourne en sortie le point Q=d.P.

L'algorithme " double and add " comporte les 3 étapes suivantes :

1) Initialiser le point Q avec la valeur P
2) Pour i allant de t-1 à 0 exécuter :
   2a) Remplacer Q par 2Q
   2b) Si d(i)=1 remplacer Q par Q+P
3) Retourner Q.

Il est apparu que l'implémentation sur carte à puce d'un algorithme de chiffrement à clé publique du type courbe elliptique était vulnérable à des attaques consistant en une analyse différentielle de consommation de courant permettant de retrouver la clé privée de déchiffrement. Ces attaques sont appelées attaques DPA, acronyme pour Differential Power Analysis. Le principe de ces attaques DPA repose sur le fait que la consommation de courant du microprocesseur exécutant des instructions varie selon la donnée manipulée.

En particulier, lorsqu'une instruction manipule une donnée dont un bit particulier est constant, la valeur des autres bits pouvant varier, l'analyse de la consommation de courant liée à l'instruction montre que la consommation moyenne de l'instruction n'est pas la même suivant que le bit particulier prend la valeur 0 ou 1. L'attaque de type DPA permet donc d'obtenir des informations supplémentaires sur les données intermédiaires manipulées par le microprocesseur de la carte lors de l'exécution d'un algorithme cryptographique. Ces informations supplémentaires peuvent dans certain cas permettre de révéler les paramètres privés de l'algorithme de déchiffrement, rendant le système cryptographique non sûr.

Dans la suite de ce document on décrit un procédé d'attaque DPA sur un algorithme de type courbe elliptique réalisant une opération du type multiplication scalaire d'un point P par un entier d, l'entier d étant la clé secrète. Cette attaque permet de révéler directement la clé secrète d. Elle compromet donc gravement la sécurité de l'implémentation de courbes elliptiques sur une carte à puce.

La première étape de l'attaque est l'enregistrement de la consommation de courant correspondant à l'exécution de l'algorithme " double and add " décrit précédemment pour N points distincts P(1),…, P(N). Dans un algorithme à base de courbes elliptiques, le microprocesseur de la carte à puce va effectuer N multiplications scalaires d.P(1),…,d.P(N).

Pour la clarté de la description de l'attaque, on commence par décrire une méthode permettant d'obtenir la valeur du bit d(t-1) de la clé secrète d, où (d(t),d(t-1),…, d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. On donne ensuite la description d'un algorithme qui permet de retrouver la valeur de d.

On groupe les points P(1) à P(N) suivant la valeur du dernier bit de l'abscisse de 4.P, où P désigne un des points P(1) à P(N). Le premier groupe est constitué des points P tels que le dernier bit de l'abscisse de 4.P est égal à 1.

Le second groupe est constitué des points P tels que le dernier bit de l'abscisse de 4.P est égal à 0. On calcule la moyenne des consommations de courant correspondant à chacun des deux groupes, et on calcule la courbe de différence entre ces deux moyennes.

Si le bit d(t-1) de d est égal à 0, alors l'algorithme de multiplication scalaire précédemment décrit calcule et met en mémoire la valeur de 4.P. Cela signifie que lors de l'exécution de l'algorithme dans une carte à puce, le microprocesseur de la carte va effectivement calculer 4.P. Dans ce cas, dans le premier groupe de message le dernier bit de la donnée manipulée par le microprocesseur est toujours à 1, et dans le deuxième groupe de message le dernier bit de la donnée manipulée est toujours à 0. La moyenne des consommations de courant correspondant à chaque groupe est donc différente. Il apparaît donc dans la courbe de différence entre les 2 moyennes un pic de différentiel de consommation de courant.

Si au contraire le bit d(t-1) de d est égal à 1, l'algorithme d'exponentiation décrit précédemment ne calcule pas le point 4.P. Lors de l'exécution de l'algorithme par la carte à puce, le microprocesseur ne manipule donc jamais la donnée 4.P. Il n'apparaît donc pas de pic de différentiel de consommation.

Cette méthode permet donc de déterminer la valeur du bit d(t-1) de d.

L'algorithme décrit dans le paragraphe suivant est une généralisation de l'algorithme précédant. Il permet de déterminer la valeur de la clé secrète d :

On définit l'entrée par N points notés P(1) à P(N) correspondant à N calculs réalisés par la carte à puce et la sortie par un entier h.

Ledit algorithme s'effectue de la manière suivante en trois étapes.

1) Exécuter h=1 ;
2) Pour i allant de t-1 à 1, exécuter :
   2)1) Classer les points P(1) à P(N) suivant la valeur du dernier bit de l'abscisse de (4*h).P ;
   2)2) Calculer la moyenne de consommation de courant pour chacun des deux groupes ;
   2)3) Calculer la différence entre les 2 moyennes ;
   2)4) Si la différence fait apparaître un pic de différentiel de consommation, faire h=h*2 ; sinon faire h=h*2+1 ;
3) Retourner h.

L'algorithme précédent fournit un entier h tel que d=2*h ou d=2*h+1. Pour obtenir la valeur de d, il suffit ensuite de tester les deux hypothèses possibles.

L'attaque de type DPA décrite permet donc de retrouver la clé privée d.

Le procédé de l'invention consiste en l'élaboration de trois contre-mesures permettant de se prémunir contre l'attaque DPA précédemment décrite.

Le procédé de la première contre-mesure consiste à calculer à partir de la clé privée d et du nombre de points n de la courbe elliptique un nouvel entier de déchiffrement d', tel que le déchiffrement d'un message chiffré quelconque avec d' donne le même résultat qu'avec d.

Dans le cas d'un algorithme cryptographique basé sur l'utilisation de courbes elliptiques réalisant l'opération Q=d.P où d est la clé privée et P un point de la courbe, le calcul de Q=d.P est remplacé par le procédé suivant en quatre étapes:

1) Détermination d'un paramètre de sécurité s, dans la pratique on peut prendre s voisin de 30.

2) Tirage d'un nombre aléatoire k compris entre 0 et 2^s;

3) Calcul de l'entier d'=d+k*n;

4) Calcul de Q=d'.P.

Le procédé de la première contre-mesure comprend deux variantes qui concernent la mise à jour de l'entier d'. La première variante consiste en ce qu'un nouvel entier de déchiffrement d'est calculé à chaque nouvelle exécution de l'algorithme de déchiffrement, selon le procédé décrit précédemment. La seconde variante consiste en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement. Lorsque ce compteur atteint une valeur fixée T, un nouvel entier de déchiffrement d' est calculé selon le procédé décrit précédemment, et le compteur est remis à zéro. Dans la pratique, on peut prendre T=16.

Le procédé de la première contre-mesure rend donc l'attaque DPA précédemment décrite impossible en changeant d'entier d de déchiffrement.

Le procédé de la deuxième contre-mesure s'applique à la première classe de courbes précedemment décrites, c'est à dire les courbes définies sur le corps fini GF(p) ayant pour équation y^2=x^3+ax+b. Le procédé de la deuxième contre-mesure consiste à utiliser un module de calcul aléatoire à chaque nouvelle exécution. Ce module aléatoire est de la forme p'= p*r où r est un entier aléatoire. L'opération de multiplication scalaire Q=d.p réalisée dans un algorithme à base de courbe elliptique s'effectue alors selon le procédé suivant en cinq étapes:

1) Détermination d'un paramètre de sécurité s; dans la pratique, on peut prendre s voisin du nombre 60;

2) Tirage du nombre aléatoire r dont la représentation binaire fait s bits;

3) Calcul de p'=p*r;

4) Exécuter l'opération de multiplication scalaire Q=d.P, les opérations étant effectuées modulo p";

5) Effectuer l'opération de réduction modulo p des coordonnées du point Q.

Le procédé de la seconde contre-mesure comprend deux variantes qui concernent la mise à jour de l'entier r. La première variante consiste en ce qu'un nouvel entier r est calculé à chaque nouvelle exécution de l'algorithme de déchiffrement, selon le procédé décrit précédemment. La seconde variante consiste en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement. Lorsque ce compteur atteint une valeur fix »e T, un nouvel entier r est calculé selon le procédé décrit précédemment, et le compteur est remis à zéro.. Dans la pratique, on peut prendre T+16.

Le procédé de la troisième contre-mesure consiste à « masquer » le point P sur lequel on veut appliquer l'algorithme de multiplication scalaire en lui ajoutant un point aléatoire R.

Le procédé de multiplication scalaire d'un point P par un entier d suivant Q=d.P comprend les cinq étapes suivantes:

1) Tirage d'un point aléatoire R sur la courbe;

2) Calcul de P'=P+R;

3) Opération de multiplication scalaire Q'=d.P';

4) Opération de multiplication scalaire S=d.R;

5) Calcul de Q=Q'- S.

Le procédé de la troisième contre-mesure comprend trois variantes. la première variante consiste en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement. Lors de la première exécution de l'algorithme de déchiffrement, l'algorithme est exécuté suivant le procédé en cinq étapes décrit précédemment. Tant que le compteur n'a pas atteint la valeur limite T, les étapes 1 et 4 du procédé décrit précédemment ne sont pas exécutées, les points R et S gardant les valeurs prises lors de l'exécution précédente. Lorsque le compteur atteint la valeur limite T, l'algorithme de déchiffrement s »effectue suivant le procédé décrit précédemment en cinq étapes, et le compteur est remis à zéro. Dans la pratique, on peut prendre T=16.

La deuxième variante consiste en ce que la carte possède initialement en mémoire deux points de la courbe elliptique tels que S=d.R. Les étapes 1 et 4 de l'algorithme de déchiffrement précédent sont remplacées par les étapes 1' et 4' suivantes:

1') Remplacer R par 2.R:

4') Remplacer S par 2.S.

La troisième variante consiste en une modification de la deuxième variante caractérisée en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement. Lors de la première exécution de l'algorithme de déchiffrement, l'algorithme est exécuté suivant le procédé en cinq étapes de la deuxième variante décrit précédemment. Tant que le compteur n'a pas atteint une valeur limite T, les étapes 1' et 4' du procédé décrit précédemment ne sont pas exécutées, les points R et S gardant les valeurs prises lors de l'exécution précédente. Lorsque le compteur atteint une valeur limite T, l'algorithme de déchiffrement s'effectue suivant le procédé précédemment décrit en cinq étapes, et le compteur est remis à zéro. Dans la pratique, on peut prendre T=16.

L'application des trois procédés de contre-mesure précédents permet de protéger tout l'algorithme cryptographique basé sur les courbes elliptiques contre l'attaque DPA précédemment décrit. Les trois contre-mesures présentées sont de plus compatibles entre elles: il est possible d'appliquer à l'algorithme de déchiffrement RSA une, deux ou trois des contre-mesures décrites.

REVENDICATIONS

1- Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé publique basé sur l'utilisation des courbes elliptiques consistant à calculer à partir de la clé privée d et du nombre de points n de ladite courbe elliptique un nouvel entier de déchiffrement d' tel que le déchiffrement d'un message chiffré quelconque, aumoyen d'un algorithme de déchiffremet, avec d' donne le même résultat qu'avec d, en réalisant l'opération Q=d*P, P étant un point de la courbe, procédé caractérisé en ce qu'il comprend quatre étapes:

1) Détermination d'un paramètre de sécurité s, dans la pratique on peut prendre s voisin de 30;
2) Tirage d'un nombre aléatoire k compris entre 0 et 2^s;

3) Calcul de l'entier d'=d+k*n;

4) Calcul de Q=d'.P.

2- Procédé de contre-mesure selon la revendication 1 caractérisé en ce qu'une première variante consiste en ce qu'un nouvel entier de déchiffrement d' est calculé à chaque nouvelle exécution de l'algorithme de déchiffrement.

3- Procédé de contre-mesure selon la revendication 1 caractérisé en ce qu'une seconde variante consiste en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'agorithme de déchiffrement jusqu'à atteindre une valeur fixée T.

4- Procédé de contre-mesure selon la revendication 3 caractérisé en ce qu'une fois la valeur T atteinte, un nouvel entier de chiffrement est calculé selon le procédé de la revendication 1 et le compteur est remis à zéro.

5- Procédé de contre-mesure selon la revendication 3 caractérisé la valeur T est égale à l'entier seize.

6- Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé publique basé sur l'utilisation des courbes elliptiques définies sur un corps fini GF(p), p étant un nombre premier, ayant pour équation y^2=x^3+ax+b, consistant à utiliser un module de calcul aléatoire à chaque nouvelle exécution de la forme p'=p*r où r est un entier aléatoire et présentant un point P caractérisé en ce que ledit procédé exécute l'opération de multiplication scalaire en cinq étapes:

1) Détermination d'un paramètre de sécurité s; dans la pratique, on peut prendre s voisin du nombre 60;
2) Tirage du nombre aléatoire r dont la représentation binaire fait s bits;
3) Calcul de p'=p*r;
4) Exécuter l'opération de multiplication scalaire Q=d.P, les opérations étant effectuées modulo p';
5) Effectuer l'opération de réduction modulo p des coordonnées du point Q.

7- Procédé de contre-mesure selon la revendication 6 caractérisé en ce qu'un nouvel entier est calculé à chaque nouvelle exécution de l'algorithme de déchiffrement.

8- Procédé de contre-mesure selon la revendication 6 caractérisé en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement.

9- Procédé de contre-mesure selon la revendication 8 caractérisé en ce que le compteur est remis à zéro lorsqu'il a atteint une valeur T.

10- Procédé de contre-mesure selon la revendication 8 ou la revendication 9 caractérisé en ce que la valeur T est égale à seize.

11. Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé publique basé sur l'utilisation des courbes elliptiques consistant à calculer à partir de la clé privée d et du nombre de points n de ladite courbe elliptique un nouvel éntier de déchiffrement d' tel que le déchiffrement d'un message chiffré quelconque, aumoyen d'un algorithme de déchiffremet, avec d' donne le même résultat qu'avec d, en réalisant l'opération Q=d*P, P étant un point de la courbe sur lequel est appliqué l'algorithme de multiplication scalaire en lui ajoutant un point aléatoire R par un entier d suiavant l'équation Q=d*P, procédé caractérisé en ce qu'il comprend cinq étapes suivantes:

1) Tirage d'un point aléatoire R sur la courbe;

2) Calcul de P'=P+R;

3) Opération de multiplication scalaire Q'=d.P';

4) Opération de multiplication scalaire S=d.R;

5) Calcul de Q=Q'- S.

12- Procédé de contre-mesure selon la revendication 12 caractérisé en ce qu'un compteur est incrémenté à chaque nouvelle

exécution de l'algorithme de déchiffrement jusqu'à une valeur T.

13- Procédé de contre-mesure selon la revendication 12 caractérisé en ce que le compteur est remis à zéro une fois atteint la valeur T.

14- Procédé de contre-mesure selon la revendication 12 caractérisé en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement jusqu'à une valeur T.

15- Procédé de contre-mesure selon la revendication 11 caractérisé en ce que la courbe elliptique possède en mémoire deux points tels que S=d*R, les étapes 1 et 4 étant alors remplacé par les étapes 1' et 4':

1') Remplacer R par 2.R:

4') Remplacer S par 2.S.

16- Procédé de contre-mesure selon la revendication 15 caractérisé en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement jusqu'à une valeur T.

17- Procédé de contre-mesure selon la revendication 15 caractérisé en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement jusqu'à une valeur T.

INTERNATIONAL SEARCH REPORT

Inter [redacted]pplication No
PCT/FR 00/00723

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	PAUL KOCHER ET AL.: "Introduction to Differential Power Analysis and Related Attacks" RETRIEVED FROM INTERNET: <URL: HTTP://WWW.CRYPTOGRAPHY.COM/DPA/TECHNICAL/INDEX.HTML> ON 24 FEBRUARY 2000; AVAILABLE ON INTERNET SINCE 1998, pages 1-8, XP002132318 San Francisco, CA, USA page 7 -page 8	1,2,6,7, 11,15

-/--

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 June 2000	09/06/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Zucka, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 00/00723

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MENKUS B: "Two important data encryption structures reported broken in record times" EDPACS, JAN. 1999, AUERBACH PUBLICATIONS, USA, vol. 26, no. 7, pages 15-18, XP000884687 ISSN: 0736-6981 page 18 ---	1,2,6,7, 11,15
A	KOCHER P C: "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems" ADVANCES IN CRYPTOLOGY - CRYPTO'96. 16TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, ADVANCES IN CRYPTOLOGY - CRYPTO '96, SANTA BARBARA, CA, USA, 18-22 AUG. 1996, pages 104-113, XP000626590 1996, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-61512-1 page 110, last paragraph -page 112, paragraph 2 ---	1,2,6,7, 11,15
A	KOBLITZ N: "Elliptic curve cryptosystems" MATHEMATICS OF COMPUTATION, JAN. 1987, USA, vol. 48, no. 177, pages 203-209, XP000671098 ISSN: 0025-5718 page 203 -page 205 -----	1,6,11, 15

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Dem [redacted] nationale No
PCT/FR 00/00723

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	PAUL KOCHER ET AL.: "Introduction to Differential Power Analysis and Related Attacks" RETRIEVED FROM INTERNET: <URL: HTTP://WWW.CRYPTOGRAPHY.COM/DPA/TECHNICAL/ INDEX.HTML> ON 24 FEBRUARY 2000; AVAILABLE ON INTERNET SINCE 1998, pages 1-8, XP002132318 San Francisco, CA, USA page 7 -page 8 --- -/--	1,2,6,7, 11,15

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
2 juin 2000	09/06/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Zucka, G

RAPPORT DE RECHERCHE INTERNATIONALE

Internationale No
PCT/FR 00/00723

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
X	MENKUS B: "Two important data encryption structures reported broken in record times" EDPACS, JAN. 1999, AUERBACH PUBLICATIONS, USA, vol. 26, no. 7, pages 15-18, XP000884687 ISSN: 0736-6981 page 18	1,2,6,7, 11,15
A	KOCHER P C: "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems" ADVANCES IN CRYPTOLOGY - CRYPTO'96. 16TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, ADVANCES IN CRYPTOLOGY - CRYPTO '96, SANTA BARBARA, CA, USA, 18-22 AUG. 1996, pages 104-113, XP000626590 1996, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-61512-1 page 110, dernier alinéa -page 112, alinéa 2	1,2,6,7, 11,15
A	KOBLITZ N: "Elliptic curve cryptosystems" MATHEMATICS OF COMPUTATION, JAN. 1987, USA, vol. 48, no. 177, pages 203-209, XP000671098 ISSN: 0025-5718 page 203 -page 205	1,6,11, 15

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)